NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

USING THE ACQUISITION PROCESS TO REDUCE THE VULNERABILITY OF FUTURE SYSTEMS TO INFORMATION WARFARE

by

William S. Mullis

March, 1997

Thesis Advisor Keith F. Snider

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 1997	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE USING THE ACQUISITION PROCESS TO REDUCE THE VULNERABILITY OF FUTURE SYSTEMS TO INFORMATION WARFARE	5. FUNDING NUMBERS
6. AUTHOR(S) Mullis, William S.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

Information warfare (IW) is a growing concern for the United States Army. The sophisticated, high-technology modern weapons systems upon which the U.S. Army heavily relies are increasing vulnerable to IW weapons and tactics. The acquisition process plays a major role in reducing defense systems' IW vulnerability. This research identifies the primary IW threats to systems during the acquisition lifecycle and what factors in the acquisition environment contribute to IW vulnerability. This research also suggests a technique for integrating IW countermeasures into the defense systems acquisition process. A primary finding of this research is that while a Program Management Office (PMO) can institute a myriad of useful countermeasures, influencing the prime contractor to establish a secure development environment is the most important action it can take in reducing the vulnerability of future systems to IW.

14. SUBJECT TERMS Information Warfare, Defense Systems Acquisition Process, Risk Management			15. NUMBER OF PAGES 79
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

Approved for public release; distribution is unlimited.

USING THE ACQUISITION PROCESS TO REDUCE THE VULNERABILITY OF FUTURE SYSTEMS TO INFORMATION WARFARE

William S. Mullis
Major, United States Army
B.S., University of Arkansas at Little Rock, 1985

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1997

Author: _____
William S. Mullis

Approved by: _____
Keith F. Snider, Thesis Advisor

_____
Dan C. Boger, Associate Advisor

_____ for
Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

Information warfare (IW) is a growing concern for the United States Army. The sophisticated, high-technology modern weapons systems upon which the U.S. Army heavily relies are increasingly vulnerable to IW weapons and tactics. The acquisition process plays a major role in reducing defense systems' IW vulnerability. This research identifies the primary IW threats to systems during the acquisition lifecycle and what factors in the acquisition environment contribute to IW vulnerability. This research also suggests a technique for integrating IW countermeasures into the defense systems acquisition process. A primary finding of this research is that while a Program Management Office (PMO) can institute a myriad of useful countermeasures, influencing the prime contractor to establish a secure development environment is the most important action it can take in reducing the vulnerability of future systems to IW.

TABLE OF CONTENTS

I. INTRODUCTION

"We live in an age that is driven by information. Technological breakthroughs...are *changing the face of war* and how we prepare for war."

- William Perry, Secretary of Defense

A. PURPOSE

The purposes of this research paper are: to analyze the current Department of Defense (DOD) and Department of the Army (DA) acquisition environment from a defensive information warfare (DIW) perspective, to identify information warfare (IW) threats during the acquisition process and to present measures that may be taken during an acquisition program to reduce vulnerabilities to IW. Specifically, current policies, regulations and procedures will be assessed for sufficient guidance and emphasis on DIW issues throughout the entire product lifecycle. Additionally, a heuristic for employing safeguards against the IW threat in the various phases of an acquisition program will be submitted.

B. BACKGROUND

Information warfare is a new and nebulous concept despite the recent surge of literature, talks and conferences devoted to the subject. An expert consensus on an acceptable definition has failed to materialize. Doctrine and operational plans that fully integrate IW into modern warfighting are also still immature and incomplete. IW first emerged as a important topic shortly after the Gulf War. After that experience the senior Army leadership began to formulate a vision of dominant battlefield knowledge (DBK)

and of drastically shortening our decision cycle while hindering or corrupting our adversaries' decision making processes. These capabilities hinge on leveraging information technology (IT) throughout our fighting force. Information and the ability to process and distribute it have become the military's and nation's "center of gravity." This realization has fueled the exploration of IW opportunities and vulnerabilities.

The United States Military is exceptionally vulnerable to IW because it has built its forces around technologically sophisticated weapons, command and control systems and a logistics support infrastructure, all of which are heavily dependent on IT. This chink in America's armor has not gone unnoticed by its enemies. A 1996 GAO report entitled *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* reveals some alarming statistics: DOD computer systems are attacked about 250,000 times a year. More than 65 per cent of these attacks are classified as successful. At least 120 countries have developed, or are developing, computer attack capabilities and are incorporating IW as part of their overall security strategy. In 1994 the government's Joint Security Commission called this vulnerability to IW "the major security challenge of this decade and possibly the next century." (Waller, 1995)

Proper actions during the acquisition process are the most effective means by which to meet this challenge. The strongest defense against IW is to engineer in information assurance from the start, rather than trying to add something on as an afterthought. (Magsig, 1995) The matching of specific IW threats to countermeasures that can be taken within acquisition programs forms the basis for this paper's research questions.

C. RESEARCH QUESTIONS

1. Primary Research Question

What actions can be taken during the acquisition process to reduce IW vulnerabilities?

2. Secondary Research Questions

a. What are the IW threats to defense systems during the acquisition process?

b. What conditions in the current acquisition environment contribute to IW vulnerabilities?

c. Do DOD and DA policies and procedures adequately address the IW threat?

d. What further studies are recommended based on the findings of the research?

D. SCOPE

This research will include: (1) an overview of IW including characteristics, weapons, tactics and techniques, (2) a discussion of specific IW threats to acquisition programs, (3) an analysis of the current acquisition environment for the factors that contribute to IW vulnerabilities and (4) a program of measures which, when applied, may reduce a system's vulnerability to IW throughout its lifecycle.

E. METHODOLOGY

This research paper's primary objectives are to assess the current acquisition environment from a DIW standpoint and to suggest ways to reduce defense systems' vulnerabilities to IW. The requisite knowledge about IW and the acquisition process will be gained from a literature review of sources including, but not limited to, the following:

- Published academic research papers

- Internet websites and homepages (DOD, commercial, and academic)
- Unclassified and classified Department of Defense publications
- Unclassified Department of the Army publications
- Department of Defense and Department of the Army policies and regulations

Additionally, interviews with DA personnel involved in writing and implementing DIW policies and procedures will be conducted. Their input will be crucial in synthesizing information and formulating counters to particular IW threats. This background research will allow for an examination of specific IW threats and an assessment of when in the acquisition lifecycle a system is most vulnerable to them. Current and proposed countermeasures will be paired against each of the threat/acquisition phase combinations to identify weaknesses or omissions. Where deficiencies are discovered, potential corrective actions or countermeasures will be suggested.

F. ORGANIZATION

Chapter II provides a detailed overview of IW, including its definition, description, unique characteristics and fundamental objectives. Next it discusses IW peculiar weapons, techniques and tactics. Chapter II also provides background information on the several phases of an acquisition program, from pre-milestone 0 through Phase III and the functions performed in each.

Chapter III identifies specific IW threats that an acquisition program may face. The chapter then provides an assessment of the current acquisition environment from a DIW perspective and presents areas of vulnerability.

Chapter IV begins with a discussion of the premier Army DIW program for tactical systems. The chapter then outlines a generalized IW vulnerability reduction heuristic that may be employed by a program manager. IW threats are matrixed across the acquisition phases and process functions along with measures or actions that may be taken to lessen the impact of IW.

Chapter V summarizes the findings of the research, restates and answers the research questions and presents recommendations for further study.

G. BENEFITS OF STUDY

The primary benefit of this research will be the vulnerability reduction heuristic developed in Chapter IV. The heuristic will enable Program Managers to make more informed decisions about the DIW issues surrounding their programs. This study will provide a framework upon which further measures can be added and additional refinements can be made as more tools and resources become available. The heightened awareness of IW resulting from this research may become the catalyst for a desperately needed closer commercial-military cooperative effort towards DIW.

II. INFORMATION WARFARE AND SYSTEMS ACQUISITION BACKGROUND

A. INTRODUCTION

The purpose of this chapter is to provide the reader with a basic understanding of IW and the systems acquisition process. Knowledge of these two subject areas is key to understanding how vulnerabilities to IW can be reduced or eliminated by actions taken in an acquisition program.

The rapid advancements in computer and telecommunication technologies made over the past couple of decades have generated tremendous warfighting capabilities for the United States Military. These technological advancements have greatly increased the lethality of modern weapons, provided instantaneous and ubiquitous communications and almost completely lifted the "fog of war" from the battlefield. All of these capabilities are dependent on information processing, dissemination and storage. It is the overarching importance of information technologies to our warfighting capacity that has changed the way we conduct operations and that has given rise to the concept of IW.

It is interesting to note that the rapid pace of technological advancements has also necessitated a change in the way we procure weapons and other defense systems. The rate of technological change was rendering systems obsolete too soon after their initial fielding. The acquisition process in recent years has been streamlined in order to shorten the time it takes to develop and field a new system. While the acquisition process has adapted to meet the reality of today's fast-paced technological advancements, it has not adapted to meet the IW threat.

B. INFORMATION WARFARE OVERVIEW

> Information warfare, in its essence, is about *ideas and epistemology*--big words meaning that information warfare is about the way humans think and, more importantly, the way humans make decisions. And although information warfare would be waged largely, but not entirely, through the communication nets of a society or its military, it is fundamentally not about satellites, wires, and computers. It is about influencing human beings and the decisions they make.
>
> -Professor George J. Stein, Air War College

1. Definition and Major Focus Areas

There is no universally agreed-upon definition of IW, but the most relevant one to this paper's subject is found in the Army's field manual, FM 100-6 *Information Operations*: "Information warfare is actions taken to achieve information superiority by affecting adversary information, information-based processes and information systems, while defending one's own information, information-based processes and information systems." This definition is very broad-based and reflects the opinion of some IW experts who believe IW should not be narrowly defined. One of the leading IW experts, Dr. Martin Libicki of the National Defense University, maintains that IW is not a single entity, but actually encompasses a group of traditional warfighting functional forms as well as several newly emerging warfare areas. The more traditional forms include command and control warfare (C2W), electronic warfare (EW) and psychological warfare (PSYCW). The developing warfare forms that he identifies as components of IW are: intelligence-based warfare (IBW), economic information warfare (EIW), hacker warfare and cyberwarfare. (Libicki, 1996)

2. Description

The above definition is also broad enough to warrant a more detailed description of IW. A better understanding of IW can be gained from a discussion of its unique characteristics, how it is categorized and who will employ it.

a. Characteristics

1. Information warfare is cheap. All that is really required is a computer and a modem. There is no need for a supercomputer or even a large mainframe. Workstations and personal computers (PC) have sufficient power to run automated system attack software. This makes entry costs extremely low. Computer and telecommunication expertise is also needed, but not necessarily expensive to obtain. A significant body of knowledge about telecommunication and computer security weaknesses already exists on the Internet. This information is free to anyone with an Internet connection. Knowledge and expertise may become less important as more and more "point and click" automated attack tools, become freely available.

2. Information-based attacks are difficult to detect and predict. Good information warriors are stealthy. Attacks may be disguised as normal operational glitches. Some operations may go completely unnoticed if the attacker simply looks at data without attempting to destroy or modify files. Inserted malicious software can remain hidden for long periods of time before being activated for attack purposes. Traditional indicators of an impending attack such as troop movements or increased message traffic are not present before an IW attack. While the tasks of detecting or

predicting attacks are difficult ones, identifying the attacker can be an almost impossible endeavor. This makes deterrence even more difficult.

3. Traditional boundaries are blurred by IW. The limits between criminal activity and acts of war are difficult to distinguish. An important example of this for the acquisition community would be the limits between industrial spying, espionage and sabotage. Other boundaries such as geographic boundaries between nations become less relevant and more ambiguous. (Rand, 1995)

4. Information warfare attacks can be conducted remotely. Computer attacks can easily be orchestrated from anywhere in the world at anytime. The battlefield will be anywhere that computer systems allow network access through any type of telecommunications media. (Irvine, 1995)

b. Categories

From the definition of IW at the beginning of the chapter it is apparent that IW operations can be categorized as either offensive or defensive. Defensive actions encompass efforts to protect against, detect and react to IW attacks. Offensive actions focus on destruction, disruption and degradation of information and information processes. Additionally, IW operations can be categorized by levels of war. IW can be conducted at either the strategic or tactical/operational level of a conflict. The primary difference between the two levels is their target sets. Strategic attacks primarily target the National Information Infrastructure (NII) and tactical attacks mainly target the battlefield operating systems (BOS). A combination of these components yields four general IW categories. A breakdown of the categories and short examples of each follow.

1. Strategic-Offensive. Attempts to alter public opinion, such as attacks against national financial, transportation, or telecommunication infrastructure, would be examples of strategic-offensive IW. Generally speaking, most strategic IW targets are civilian and not military in nature.

2. Strategic-Defensive. Any effort to secure national telecommunications infrastructure, define national systems security standards, or to establish national damage control mechanisms, such as a national Computer Emergency Response Team (CERT), would qualify as strategic-defensive IW.

3. Tactical-Offensive. Actions that fit into the tactical-offensive category includes disruption or destruction of battlefield commanders' (theater level and below) communication and intelligence networks, battlefield deception operations and the use of soft kill techniques against specific weapon systems.

4. Tactical-Defensive. Network security measures, battlefield encryption, anti-jamming and anti-intercept techniques are all examples of tactical-defensive IW.

Figure 1 shows the breakdown and summarizes the operational focuses of each category. There is some gray area between what constitutes a strategic attack versus a tactical one. An IW attack against the national air traffic control system with the purpose to delay the deployment of troops to a theater of operations could be classified as either strategic or tactical. The primary focus of this research is in the defensive-tactical area.

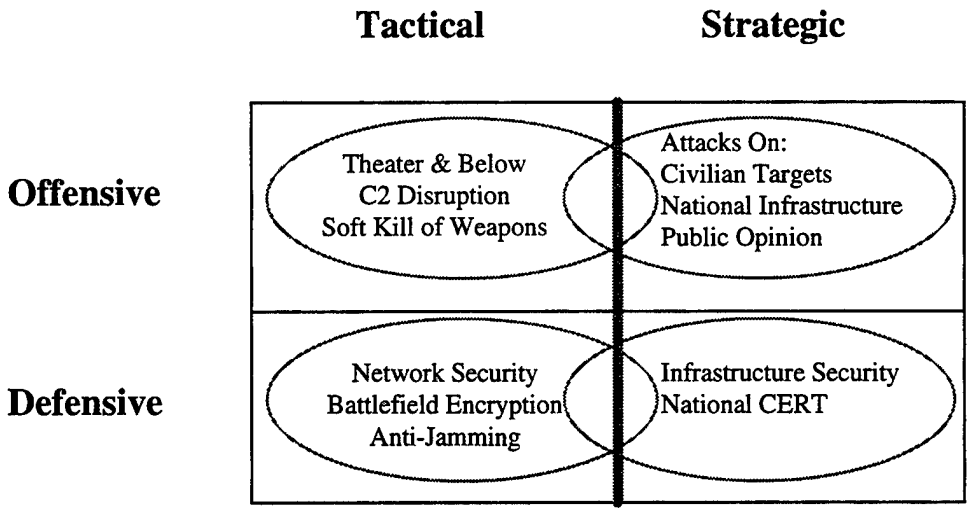

Figure 1-1, IW Operations Matrix

c. Potential Adversaries

Because of the low entry cost, difficulty in detection, capability to conduct strikes remotely and blurred boundaries, IW is an attractive option for both terrorists and criminals. Terrorists can continue to operate much as they always have, but with the added benefits of inexpensive, reusable weapons and blurred legal boundaries which may hinder prosecution or retaliatory actions. Criminal hackers enjoy much the same benefits. The ability to commit a crime from great distances with little chance of detection could be a boon to criminal activity.

Beyond terrorists and rogue hackers looms the even greater threat of nations conducting organized, coordinated IW operations against the United States. The effective, inexpensive IW option is most advantageous to small, developing countries which cannot compete with the U.S. conventional force structure. IW gives even a tiny nation the ability to project power into the heart of America. However, any foe, large or

small could significantly increase its warfighting capacity by combining traditional combat operation with IW operations.

C. INFORMATION WARFARE WEAPONS AND EFFECTS

Traditional, hard-kill weapons such as bombs, missiles and rockets still have a place in IW. However, a whole new set of electronic weapons are being developed to add a soft-kill capability as well as add new hard-kill options. These new IW weapons are designed to achieve three types of effects: physical, semantic or syntactic. Physical effects refer to the destruction of information processing facilities and equipment. Semantical weapons focus on destroying the trust and truth maintenance components of a system. This is mainly accomplished through carefully orchestrated perception distortion. Electronic media make possible extremely complex and convincing psychological operations. Syntactical weapons attack the operating logic of a system to introduce unpredictable behaviors or deny reliable information services to the users. (Garigue, 1996)

Semantical effects may be enhanced by IW technologies, but rely mainly on numerous proven psychological warfare and operational deception techniques. These techniques fall outside the scope of this paper. The IW weapons discussed in the remainder of this section are used mainly to achieve syntactic or physical effects, however they may be employed as part of a semantical attack. The following list of weapons (from Russell and Gangemi, 1992) is not a complete one, but contains enough typical examples to formulate a basic understanding of IW weaponry.

1. Malicious Software, Hardware and Firmware

Computer Viruses: A virus is a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces.

Worms: A worm is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually does not modify other programs.

Trojan Horses: A trojan horse is a code fragment that hides inside a program and performs a disguised function. It is a popular mechanism for disguising a virus or a worm.

Logic Bombs: A logic bomb is a type of a trojan horse, used to release a virus, a worm or some other system attack. It is either an independent program or a piece of code that has been planted by a system developer or programmer.

Trap Doors: A trap door, or back door, is a mechanism that is built into a system by its designer. The function of a trap door is to give the designer a way to sneak back into the system, circumventing normal system protection.

Chipping: Chipping is the introduction of microchips or other hardware, which are designed to fail, into a piece of equipment. The components can be designed to fail after a certain time period, upon receiving a signal, or when some set of conditions is met.

2. Energy Weapons

Electromagnetic Pulse (EMP) Generators: EMP Generators are non-nuclear devices that produce an electromagnetic energy pulse strong enough to destroy or disable electronic circuits, including integrated circuits (IC).

High Energy Radio Frequency (HERF) Guns: HERF Guns produce effects similar to EMP Generators. They overload, degrade and destroy electronic components using high energy radio waves.

3. Spoofing

Spoofing: Spoofing is sending a false message or signal. It can be accomplished by either tricking a system into believing the sender is a legitimate user or by altering a legitimate user's message. This is really more of a technique than a weapon, but it is a serious threat because there are many ways a system can be spoofed. Two of the more common forms are router and mail spoofing.

D. ACQUISITION PROCESS OVERVIEW

The following descriptive paragraphs for each of the acquisition phases are taken directly from the DOD regulation governing acquisition programs, DOD Regulation 5000.2-R. Items that have particular relevance to IW are bolded for emphasis and are discussed under each phase heading. All programs, including highly sensitive, cryptologic and intelligence programs, shall accomplish certain core activities described in DODD 5000.1 and DOD Regulation 5000.2-R. These activities are accomplished in phases.

Some tailoring of activities, decision points and phases can be made to meet the specific needs of a program manager and as a cost reduction measure. (5000.2-R, 1996)

1. Pre-Milestone 0

All acquisition programs are based on identified, documented and validated mission needs. Mission needs result from ongoing **assessments** of current and projected capability.

This assessment is called a Mission Area Analysis (MAA). Its major purpose is to identify warfighting deficiencies. A Mission Needs Statement (MNS) is produced from the MAA. It describes a operational need in terms of a general capability, i.e., a capability to destroy deeply buried, hardened targets. It also describes what kind of environment the system must operate in and what type of weapons and attacks it must be able to survive. The Operational Requirements Definition (ORD) is developed from the MNS. The ORD establishes the system's Measures of Performance (MOP). The quantitative performance standards for the system are detailed in the ORD.

2. Phase 0: Concept Exploration

Phase 0 typically consists of competitive, parallel short-term concept studies. The focus of these efforts is to define and evaluate the feasibility of alternative concepts and to provide a basis for assessing the relative merits of these concepts at the next milestone decision point. Analysis of alternatives shall be used as appropriate to facilitate comparisons of alternative concepts. The most promising system concepts shall be defined in terms of initial, broad objectives for cost, schedule, **performance, software**

requirements, opportunities for tradeoffs, overall acquisition strategy and **test and evaluation strategy**.

Software performance parameters are where systems security issues must be addressed. The test and evaluation strategy has to include software testing, not only for performance, but also for intentionally-inserted malicious code.

3. Phase 1: Program Definition and Risk Reduction

During this phase, the program shall become defined as one or more concepts, design approaches, and/or parallel technologies are pursued as warranted. Assessments of the advantages and disadvantages of alternative concepts shall be refined. Prototyping, demonstrations and early operational assessments shall be considered and included as necessary to reduce risk so that technology, manufacturing and support risks are well in hand before the next decision point. Cost drivers, lifecycle cost estimates, cost-performance trades, **interoperability** and acquisition strategy alternatives shall be considered to include **evolutionary** and **incremental software development.**

Interoperability requirements often demand additional security measures. The choice of software development methodologies, waterfall, incremental, or evolutionary, impacts on the systems security design. One methodology may provide significant advantages or disadvantages to the security requirements plan.

4. Phase 2: Engineering Manufacturing Development/Low Rate Initial Production

The primary objectives of this phase are to: translate the most promising design approach into a stable, interoperable, producible, supportable and cost-effective design; validate the manufacturing or production process; and, **demonstrate system capabilities through testing**. Low Rate Initial Production (LRIP) occurs while the Engineering and Manufacturing Development phase is still continuing as test results and design fixes or upgrades are incorporated.

Testing plays a major role in this phase. One of the major problems in traditional software testing is that we can only confirm the presence of errors; we cannot test for the absence of them. Program managers cannot be certain that zero errors exist even if testing fails to identify any "bugs". (Jones, 1996)

5. Phase 3: Production, Fielding/Deployment and Operational Support

The objective of this phase is to achieve an operational capability that satisfies mission needs. Deficiencies encountered in Developmental Test and Evaluation (DT&E) and Initial Operational Test and Evaluation (IOT&E) shall be resolved and fixes verified. (The production requirement of this phase does not apply to ACAT IA acquisition programs (ACAT IA programs are major automated information systems) or software-intensive systems with no developmental hardware components.) During fielding/deployment and throughout operational support, the **potential for modifications to the fielded/deployed system continues.**

Prior to entering this phase a system must perform to standards during DT&E and IOT&E. The DIW issue here is how to conduct vulnerability testing for software and electronic hardware. Also of concern are major modifications to a system after its initial fielding. This is another chance for malicious software or hardware insertion.

This background information provides the basic understanding of IW and the acquisition process needed to discuss the current defensive IW posture of the acquisition system.

III. ACQUISITION SYSTEM DEFENSIVE INFORMATION WARFARE POSTURE

A. INTRODUCTION

The purpose of this chapter is to document the current DIW status of the Army acquisition system. First, the two major IW threats to weapons or defense systems programs will be discussed. Second, using those threats as a basis for analysis, factors in the current acquisition environment that complicate or hamper DIW efforts will be investigated. The chapter will end with a summary and analysis of the Army's DIW plan, focusing on its application to acquisition programs.

B. INFORMATION WARFARE THREATS

Acquisition programs face two specific types of IW threats. First, the weapon or other defense system under development can be targeted. The focus of these attacks would be to degrade a system's performance sometime in the future, after its fielding to operational units. Second, the program management process can be disrupted. The intent of these attacks would be to cause a delay in system deployment or complete cancellation of a program.

1. Attacks for Future Exploitation

Systems may be procured with vulnerabilities to either physical or syntactical attacks embedded into them. These vulnerabilities may result simply from the omission of DIW requirements from the ORD, or from malicious system component alterations during design, production or post-fielding modifications. One example of this threat

would be the omission of EMP hardening requirements for critical electronic components when there is reasonable expectation that adversaries are capable of employing EMP generators. Another example would be the insertion of a trojan horse into fire control software that generated guidance errors when used in certain geographic areas or when tracking specific targets.

2. Direct Program Attacks

Information warfare attacks aimed directly against program management processes may seek to take advantage of the current economic reality. Acquisition programs today operate under extreme budgetary pressures. Moderate increases in program costs, slips in schedule or reductions in expected performance are grounds for cancellation. In this case semantic or syntactic attacks would most likely be used. An example of this type of threat would be alterations to cost or performance data which could destroy the trust between the government and the system's contractors, putting the program at risk of cancellation. Such syntactic attacks against either the civilian contractors' or government's administrative systems could cause costly delays or the complete withdrawal of Congressional support for a program.

C. CURRENT ACQUISITION ENVIRONMENT

The current acquisition environment, the product of military budget cuts and rapid technological advancement, is not conducive to DIW programs. The acquisition environment is shaped by the need to procure the most up-to-date technology, right now, at cut-rate prices. The intense effort needed to make this happen has, at worst, distracted

acquisition policy and decision makers from DIW issues or, at best, drained resources away from DIW efforts. Major problem areas are highlighted below.

1. Policy

Acquisition policy documents at the DOD and DA level do not presently address IW issues sufficiently. At the DOD policy level, DIW guidance is contained in DOD Regulation 5000.2-R in the following three sections:

4.3.5 Software Engineering

Software shall be managed and engineered using best processes and practices that are known to reduce cost, schedule and technical risks. It is DOD policy to design and develop software systems based on systems engineering principles to include:

7. Ensuring that information warfare risks have been assessed (DOD Directive TS-3600.1).

4.4.5 Program Protection

Acquisition programs shall identify elements of the program, classified or unclassified, that require protection to prevent unauthorized disclosure or inadvertent transfer of critical program technology or information. Program protection planning shall begin early in the acquisition lifecycle and be updated as required. The planning process shall incorporate risk management and threat-based countermeasures to provide cost-effective protection. When appropriately applied, the process will meet requirements of information systems security, defensive information warfare, classification management, TEMPEST, physical security, personnel security, operations security, international security, technology transfer and special access programs.

4.4.6 Information Systems Security

Information systems security requirements shall be included as part of program and systems design activities to preserve integrity, availability, and confidentiality of critical program technology and information. System security requirements shall be established and maintained throughout the acquisition lifecycle for all ACAT 1A

programs and others as applicable. All Automated Information Systems (AIS) shall meet security requirements in accordance with DODD 5200.28 and be accredited by the Designated Approving Authority prior to processing classified or sensitive unclassified data.

These sections are flawed for two reasons. First, they address only the threat of IW directed against the program management processes. The single sentence warning in the software engineering section does not provide enough guidance to Program Managers for them to protect their systems from DIW design flaws or intentional software or hardware modifications. Second the references cited; DODD TS-3600.1 and DODD 5200.28 (commonly referred to as the "Rainbow Series") are seriously outdated and flawed when applied to much of today's cutting-edge information technology.

At the DA level the situation is only slightly better. The Army acquisition regulation, AR 70-1, is currently under revision, but still does not include any reference to information warfare. However, the draft Army regulation on Information Systems Security (ISS), AR 380-19 (draft) does offer guidance for guarding against malicious software insertion and IW risk assessment. It also identifies DIW actions which could be applied to protect program management processes. Unfortunately, AR 380-19 is focused solely on AISs, not weapons systems, and the risk assessment methodology is not detailed enough. The fact that an Army regulation intended for Army-wide applicability would specifically address acquisition IW issues better than the DOD acquisition regulation highlights the problem with identifying which agencies are responsible for DIW.

2. Responsibilities

The Army is a unique organization and its solution for carving up DIW responsibilities is also unique. It is also confusing. Most major business organizations have identified the need to establish a Chief Information Officer (CIO) position. Normally, the CIO "owns" everything pertaining to the organization's IT environment including; equipment, infrastructure, training, software application packages, standards and security policy. Basically, the CIO controls everything but the data. The Army's CIO is the Director of Information Systems for Command, Control, Communications and Computers (DISC4). The DISC4 shares responsibility for the areas listed above and all the Army's information operations with the Deputy Chief of Staff for Operations (DCSOPS) and the Deputy Chief of Staff for Intelligence (DCSINT). However, the DCSOPS, not the CIO, is the leader in the Information Operations (IO) Triad. This arrangement is probably due more to historical precedent rather than any organizational design rationale. There are additional organizational issues. A prime example is the responsibility given to the Program Executive Officer for Command, Control and Communication Systems (PEO C3S). The Army Digitization Office (ADO) is to direct the PEO C3S in integrating the Army's DIW plan into the new Army force structure (Force XXI). The ADO is nowhere in the chain-of-command for PEO C3S. Further, while PEO C3S may have the majority of the digitization programs under his/her control, there are numerous other key weapons procurement programs over which he/she has no formal authority or responsibility. The bottom line is that the lack of unity of command may lead to confusion, duplication of effort, and turf battles. Possibly the most

devastating part of this arrangement is that the Army Acquisition Executive (AAE) , who has a tremendous stake and role to play in DIW, is not a member of the IO Triad, but must rely on representatives from the ODISC4 to champion his position and to keep him updated on current plans and strategy. This arrangement lessens the AAE's ability to constructively contribute in the DIW policy decision making process.

3. Acquisition Reform Measures

Many of the recent acquisition reform initiatives, while absolutely needed to shorten procurement cycle time and reduce costs, contribute to our IW vulnerabilities. Generally speaking, acquisition reform measures call for reduced government involvement and oversight. The Military Standards (MILSTD) that previously detailed the amount and type of supervision the government expected from a defense contractor have been all but banned. Contractors must now only meet performance specifications for a new weapon. They determine and control their own design, manufacturing and testing processes. Two areas of particular concern are configuration management and systems engineering. Stringent configuration management controls are critical in the effort to guard against malicious hardware and software insertion. An effective systems engineering effort is essential if systems security features are to be successfully integrated into a product.

Another reform initiative that contributes to the IW threat is the preference for Commercial-Off-The-Shelf (COTS) products and Non-Development Items (NDI). COTS and NDI buys increase the risk of unauthorized modifications to hardware and software. It also allows potential enemies to take advantage of known security flaws or to readily

examine equipment for other weaknesses to exploit. The former protective measure of buying only National Computer Security Center (NCSC) evaluated products is no longer feasible. The demand has far outstripped the agency's capacity to perform product evaluations. (Vol. I, C2 Protect Library, 1995)

4. Foreign Source Components

Using components from foreign sources increases the risk that a system has been maliciously modified. The U.S. military is no longer the country's technology leader and the U.S. is no longer the world leader in many technology areas. We do depend on foreign components to keep a technology edge and to curb costs. However, many of the components we purchase are perfect for modification as part of a nation's offensive IW operations. A good example of this is the new circuit board and microprocessor built by Thomson Tubes and Computers of Grenoble, France for the M1A2 Abrams main battle tank. (McAuliffe, 1996) While the French are not traditional enemies, they are notorious for conducting extensive industrial espionage and they did provide the Iranians with the "SARI" missile system just prior to the Gulf War. It is no great leap of the imagination to believe that they could, with their government owned industries, alter components of our defense systems.

5. Vulnerability Assessment and Risk Management Tools

Current vulnerability assessment methodologies and risk management tools are designed for evaluating and mitigating risks for information systems. These tools and methodologies need constant revision to keep pace with new technologies and often do

not adequately address the most recent threat developments. New assessment and risk management techniques geared toward embedded software systems found on most modern weapons systems are being developed, but are still immature. The Communications-Electronics Command Information Operations Special Projects Office (CECOM IO SPO) is currently working on both of these areas, but the programs are still in the developmental stages. (Rabb, 1996)

6. Requirements Definition Process

The best time to address IW vulnerability issues is during the requirements definition process. This is not currently being accomplished. The System Threat Analysis (STA) should be modified to include both current, validated IW threats and probable future IW threats. The use of Integrated Product Teams (IPT) during the requirements determination stage may be an effective means of integrating DIW measures into the ORD. To be effective, the users and other decision makers must be educated about IW and IW experts must be included in the IPT.

7. Training and Education

Acquisition professionals are not adequately trained and educated in information operations or information warfare. This may be the single most critical deficiency area in the acquisition system DIW posture. Simply raising IW awareness through education and training programs would reap tremendous benefits. So much of DIW is simple Computer Security (COMSEC). Good COMSEC is largely a training problem, not a technical problem. This deficiency has been identified and IW training and education programs are

quickly being instituted. New security courses for Army system administrators and security managers were implemented on 1 October 1996. Additionally, some IW training was added to the subjects being taught at the Army's Computer Science School. However, the curriculum is mainly geared toward systems administrators and operators, not acquisition personnel.

8. Economic Constraints

The shrinking defense budget drastically limits the DIW effort. The bottom line is that there is not enough money to acquire everything the Army needs in order to establish and maintain a strong DIW posture. Training and education, additional product testing and evaluation, inclusion of DIW features in performance requirements and emergency response capabilities are all very necessary, but must compete with many other high-priority programs for funding. Detailed examples of how funding affects DIW programs will be presented later in the chapter.

9. Contracting Issues

The bottom line with contracting is that we simply do not currently address IW issues in our contracting instruments. Making program security a criteria for source selection appears to be a viable way to assist in reducing the threat of IW. (Stone, 1996) However, there are other issues involved that raise important questions in the areas of contractor liability, awards and subcontract management. The three major questions are:

1) Should we hold contractors responsible for malicious alterations made to software or hardware made by employees?

2) Should we incentivize contractors to more effectively protect themselves and their program from IW and, if so, how?

3) Should we control prime contractors' choices in subcontractors for software development, microprocessors and telecommunications components.

The blurring of legal boundaries, lack of strong criminal computer security laws and the need to use best business practices, whenever possible, complicate the answers to these questions.

10. Testing Procedures

Testing requirements contained in DOD 5000.2-R, Appendix IV (Live Fire Test and Evaluation Reports Mandatory Procedures and Formats), do address testing covered systems for vulnerability to attacks from directed energy weapons. However, LFT&E is aimed at determining crew survivability, not system suvivability. Requirements for tests to prove system survivability against energy or other IW weapons such as computer viruses or worms are not so clearly defined. Appendix III (Test and Evaluation Master Plan Mandatory Procedures and Format) does state that software must be evaluated to ensure that performance requirements are met, but there is no mention of operation in an IW threat environment. Developing the ability to simulate a hostile IW environment is a major concern. Testing hardware for survivability is well understood, but software is the major target of "soft kill weapons". How do you measure software degradation? How do you simulate a covert IW attack? How do you measure software resiliency? None of these problems are adequately addressed by current operational testing procedures.

D. ARMY DEFENSIVE INFORMATION WARFARE PROGRAM: COMMAND AND CONTROL PROTECT LIBRARY (C2 PROTECT)

1. Background

In November, 1994 ODISC4 was tasked to assist ODCSOPS in formulating a response to DISA's DIW Management Plan. Because the Army leadership is primarily concerned with tactical operations, the Army's DIW plan was to be focused on battlefield C2 systems. (Vol. I, C2 Protect Library, 1995) Therefore, an Army C2 Protect Working Group (Army C2PWG) was established to develop an Army DIW plan that would support and enhance DISA's DIW efforts. The result is the C2 Protect Library published in August, 1995. The C2 Protect Library consists of six volumes: C2 Protect Program Management Plan (Volume I), C2 Protect Master Training Management Plan (Volume II), C2 Protect Implementation Plan (Volume III), Intelligence Support to C2 Protect Action Plan (Volume IV), C2 Protect Future Year Resourcing Proposal (Volume V) and the C2 Protect Threat Document (Volume VI). (Vol. I, C2 Protect Library, 1995)

2. Purpose

The purpose of the C2 Protect Program Management Plan (PMP) is to identify the Army's C2 Protect vision, strategy, goals and responsibilities. The plan documents requirements to support C2 Protect actions for near-term, mid-term and long-term goals.

The PMP provides guidance for the identification and execution of C2 Protect management requirements in support of the Army's IO doctrine. (Vol. I, C2 Protect Library, 1995)

3. Acquisition Applicability

The C2 Protect PMP (Volume I), Master Training Plan (Volume II) and Implementation Plan (Volume III) appear to be well-structured documents which address a large portion of the major acquisition issues and IW threats.

Volume I identifies the need for Systems Security Engineering (SSE) to be integrated into the Systems Engineering process. It addresses the current deficiency in IW training and education. It also identifies the requirement for a more realistic IW/C2W testing environment. Additionally, it provides for vulnerability assessments to be conducted on developmental systems using a Red Team technique. The Red Team experts would simulate opposing force-like capabilities to expose weaknesses and recommend solutions. General DIW responsibilities of the Assistant Secretary of the Army for Research, Development and Acquisition (ASA[RDA]), who is dual-hatted as the AAE, and PEOs/PMs are given in sections 8.1 and 8.12 respectively and are listed below:

8.1 ASSISTANT SECRETARY of the ARMY FOR RESEARCH, DEVELOPMENT AND ACQUISITION (ASA [RDA]) SHALL:

1) Provide or coordinate funding for C2 Protect R&D activities.

2) Ensure C2 Protect concerns are an integral part of ASA (RDA) management systems.

3) Provide relevant C2 Protect input to the DISC4 to support Army IW policy.

4) Ensure C2 Protect requirements are integrated into ASA (RDA) information systems.

5) Coordinate with other services and defense agencies where common interests exist to minimize duplication of effort in C2W programs and

equipment development and to achieve standardization, interoperability, and compatibility in fulfilling common requirements.

6) Plan and coordinate development or procurement of simulated hostile IW/C2W systems for testing and training.

7) Conduct research and acquire basic knowledge of the techniques and circuitry required to provide an effective defensive (vulnerability assessment) IW/C2W capability in appropriate types of Army equipment. Ensure PEOs use this knowledge and share it within forums such as the Joint Directors of Laboratories (JDLs).

8) Develop a capability that shall be able to evaluate information systems risk analysis, risk reduction and risk management.

9) Ensure that Army PEOs/PMs include Systems Security Engineering Modeling in all systems development activities.

10) Review Army programs in conjunction with ODCSOPS for application to IW and advise the Assistant Secretary of Defense, Command, Control, Communications and Intelligence (ASDC3I) of the outcome of these reviews.

8.12 PEOS AND PMS SHALL:

1) Certify that their programs, projects and systems meet Army/DoD C2 Protect standards, policy and procedures.

2) Ensure funding is provided to C2 Protect for their projects.

3) Integrate System Security Engineering (SSE) processes into system design and development.

4) Integrate ISS practices into pre-milestone zero activities and events.

5) Develop and submit a C2 Protect System Security Engineering implementation plan for all transport and information systems developments for which they have design and development responsibilities.

6) Develop and perform security Risk Analysis on all systems developments before determining the omission of security features.

7) Be responsible for acquisition and lifecycle management of materiel in support of the IW/C2W strategy.

Volume III assigns specific tasks and subtasks to individuals to assist them in fulfilling their responsibilities under the PMP. The ASA(RDA) taskings are contained in Annex H:

Task 8 Define and Prioritize C2 Protect RDA Requirements

A. Task Statement

ASA (RDA) must integrate C2 Protect measures into Army systems, those systems currently under development and all future systems. In addition, SARDA must incorporate emerging information technologies throughout research, development, testing, production, fielding and life cycle support.

Concept of the Plan

ASA (RDA), in conjunction with the C2 Protect Triad, shall develop an RDA strategy to support C2 Protect. This strategy shall support the continued evolution of C2 Protect Information Technology developments, innovative approaches and efforts underway within DOD, academia and private industry. Research, Development, Test and Evaluation (RDT&E) for C2 Protect shall include investigations of the modifications required to adapt commercial hardware and software for use by the military. Technology assessments and technology demonstrations shall be accomplished to provide insights into what is possible and feasible.

ASA (RDA) must ensure that C2 Protect common tools (Task 10, Annex J) are integrated into current Army systems, those under development and all future systems incorporating emerging information technologies throughout research, development, testing, production, fielding and lifecycle support using a Risk Management Process developed under Task 12, Annex L of this plan.

B. Sub-Tasks

1) Develop RDT&E strategy to support C2 Protect. Address the requirement for future methods of protecting C4 systems. (Near-Term)
2) Coordinate C2 Protect efforts within the RDT&E community. (Near-Term)
3) Investigate and develop Intrusion Detection, Audit Reduction and Automated Reporting Technologies as required. (Near-Term)
4) Investigate MLS technologies for integration into Army information and command and control systems. (Long-Term)

5) Investigate and develop reconfiguration and reconstitution technologies. (Long-Term)

6) Develop a certification process to evaluate NDI , COTS and GOTS applications/items which have been obtained for Army-wide use. (Long-Term)

7) The RDA process will address and resolve technical interoperability problems of information and command and control systems throughout the Army environment. It will embed System Security Engineering in system acquisition, possibly using NSA's System Security Engineering model as a tool.

Volume III accomplishes two other important tasks. First, it provides a risk management process model that can be applied to a system across its lifecycle (Figure 3-1). The model, developed by Mr. Craig Rabb of CECOM , demonstrates how the validated IW threat and potential future threats determined through technology assessments influences the system requirements. It also shows that constant vulnerability assessment should lead to non-material solutions like changes in Training, Tactics and Procedures (TTP) or changes to system itself until an acceptable level of risk is achieved.

Second, it calls for the development and integration of a set of common automated protect tools, which will assist in vulnerability assessment, into all applicable Army C2 systems.

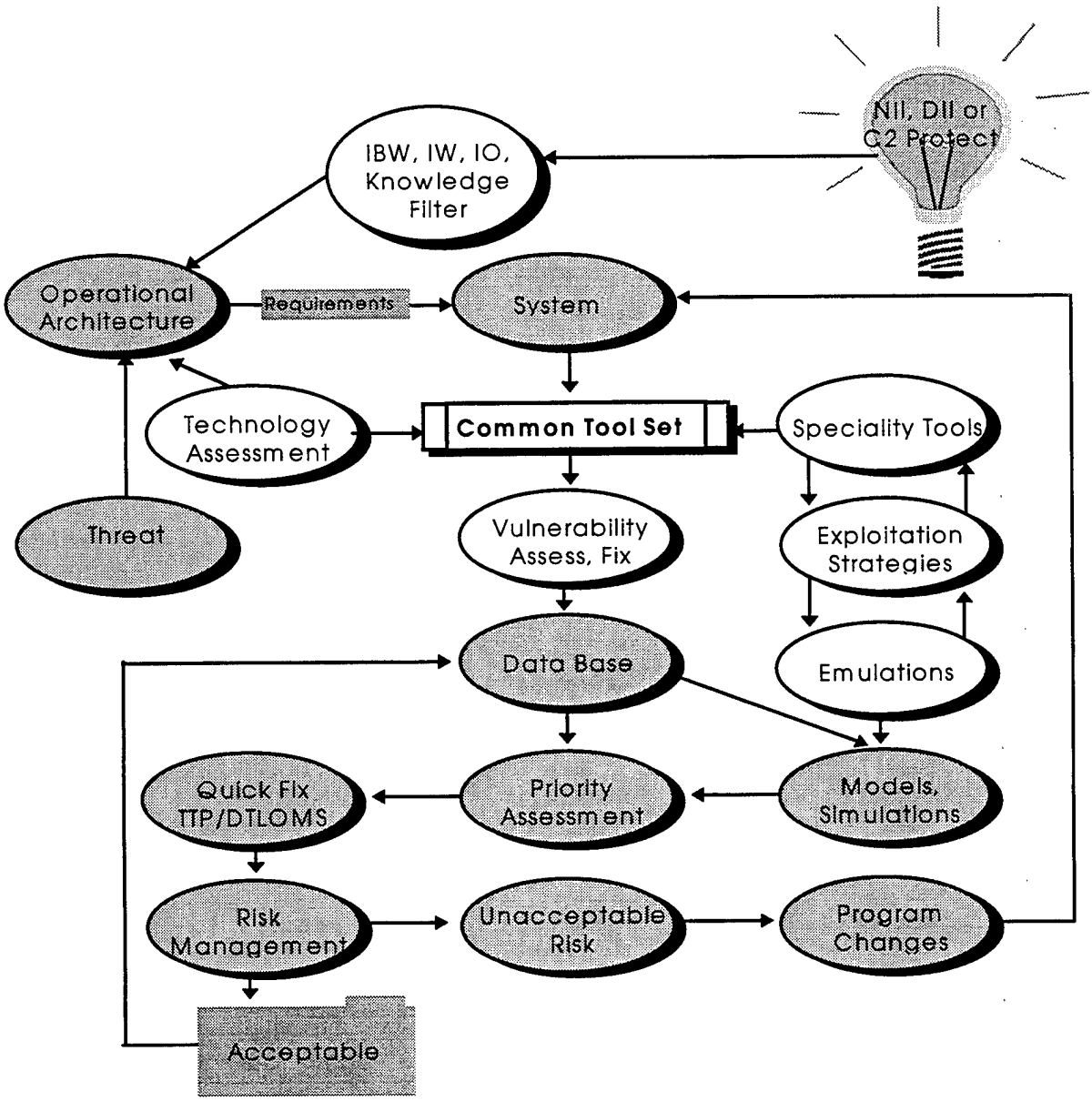

Figure 3-1, IW Risk Management Process Model from (Vol. III ,C2 Protect Library, 1996)

Volume II details specific training responsibilities for PEOs/PMs in section 7.1. These responsibilities are listed below:

7.1 The PEOS/PMS SHALL:

1) Ensure that C2 Protect training associated with the systems security engineering models is included in all systems development activities.

2) Ensure funding is provided for certification and training of personnel responsible for System Security Engineering (SSE).

3) Ensure C2 Protect training requirements are included as part of the design, development and fielding of their information systems.

4) Incorporate risk management as an integral part of C2 Protect programs, education, awareness and training.

4. Current Implementation Status

Despite the emphasis given C2 Protect activities, implementation has been slow. The Chief of Staff of the Army, General Reimer stated in a message distributed on 3 September 1996 that: "With threats to our information systems increasing daily, priority of effort in the near term will be on implementing the Army's C2 Protect Management, Training and Implementation Plan." (Reimer, 1996) Even with this backing, funding has been a severe constraint in executing C2 protect measures. The Army Information Systems Security Resource Program (ISSRP) suffered a 76% budget decrement in fiscal years (FY) 1994 and 1995. Resources remain meager through FY 2001. The resourcing shortfalls have forced C2 planners to focus on three areas; activating the Army CERT, developing the common tool set and increasing security training. Additional funding to accomplish other C2 tasks does not become available until FY 1998 and 1999. (Loranger,

1996) Additionally, the complex organizational structure has hindered implementation. As previously mentioned the ASA(RDA) is not directly represented in the IO Triad, resulting in less than perfect communication. A good example of this is the fact that the chief of policy in the ASA(RDA)'s office has not yet received the C2 Protect Library documents and therefore has no idea that he should be issuing directives and policy on DIW procedures, training and other requirements. (Waldschmidt, 1996) The chairman of the C2PWG, out of sheer necessity, has been issuing guidance directly to PEOs/PMs, circumventing the normal chain-of-command (Loranger, 1996). These execution difficulties are exacerbated by omissions in the plan itself, which are discussed next.

5. C2 Protect Shortfalls

Despite the general high quality of the C2 protect plan, it does have deficiencies other than resourcing as it pertains to the acquisition process. First, it is aimed at C2 systems exclusively, therefore the unique DIW problems associated with software and hardware embedded in weapons systems are largely ignored. Of course most, if not all, modern weapons tie into the C2 system, making them technically part of the C2 system. The C2 Protect Plan developers may have drawn their system boxes too small, excluding the "shooters". Second, after examining the C2 Protect Library, it is apparent that the authors presupposed IW attacks on a system only *after* its fielding or that vulnerabilities in a system would result only from ill-defined design requirements. Lastly, the responsibilities assigned to the acquisition community are very broad and are described in fairly general terms. Only individuals with a clear understanding of computer and network security would be able to formulate an action plan based on this guidance.

Ironically, one of the major problems identified in the C2 Protect documents is the lack of training and education. This is an observation, not a criticism. The C2 Protect volumes cannot spell out every detail and must speak in general terms on some subjects. Despite the tremendous coverage of issues in other areas, these shortfalls do leave holes in our DIW strategy. Chapter IV will address these deficiencies and suggest a methodology for correcting them.

IV. VULNERABILITY REDUCTION

A. INTRODUCTION

The purpose of this chapter is to synthesize the information presented in the previous three chapters and formulate a framework for reducing the threat of IW using actions that may be taken within the systems acquisition process. The framework will expand on and support the C2 Protect Library, exploiting the strengths of the plan and shoring-up the weaknesses. The first section of the chapter will identify a critical relationship between DIW efforts and protecting an acquisition program from its two fundamental IW threats. The second section will offer acquisition program decision-makers a heuristic for formulating an IW vulnerability reduction strategy. The final section will provide a generalized example of applying the heuristic to an acquisition program.

B. SYSTEMS ACQUISITION PROCESS: DEFENSIVE INFORMATION WARFARE RELATIONSHIPS

A careful analysis of the interaction between the two major IW threats to acquisition programs and the DIW countermeasures used against those threats reveals a couple of critical leverage points. These leverage points represent the areas where, if DIW measures are applied, the most benefit is gained.

In Chapter III the two major IW threats were identified as: 1) Direct Program Attacks, or IW operations against the program management processes of a system under development and 2) Attacks for Future Exploitation which are IW operations to

introduce vulnerabilities into a system which can be exploited later, on the battlefield. If we match-up generalized countermeasures to each of these threats an important relationship emerges.

This relationship can be compared to a piece of fruit that is being examined for use as a seed source. The meat of the fruit is protected by a skin. The skin can be likened to a contractor's or government program management office's business information security plan. The meat of the fruit represents sensitive business data which, if exposed or corrupted, would make the fruit or program appear undesirable and subject to being discarded. At the heart of the fruit is what we are truly after--the seed or product. It is protected by a hard outer shell. This is analogous to a product-specific IW vulnerability reduction plan. This protects the genetic material inside the seed itself. If the genetic material is corrupted, then weakened, vulnerable trees are produced, much like how malicious code or modified hardware may render a weapon system vulnerable. However, if the genetic material is flawed from the beginning, the hardness of the seed will not matter. The same is true with a vulnerability reduction plan. If proper DIW measures are not integrated into the design requirements, a system will be inherently vulnerable.

From this analogy it is clear that the government program office's and contractor's Management Information System (MIS) security plan is the first line of defense against the threat of Direct Program Attacks. These security plans also strengthen and augment the product-specific vulnerability reduction plan. The product- specific vulnerability reduction plan is the primary defense against Attacks for Future Exploitation. We may designate the combination of these two plans the Program Security Environment (PSE).

The PSE and the integration of DIW measures into the system design process using structured SSE techniques constitute the two major leverage points. In fact it is helpful to view their combination as a lever.

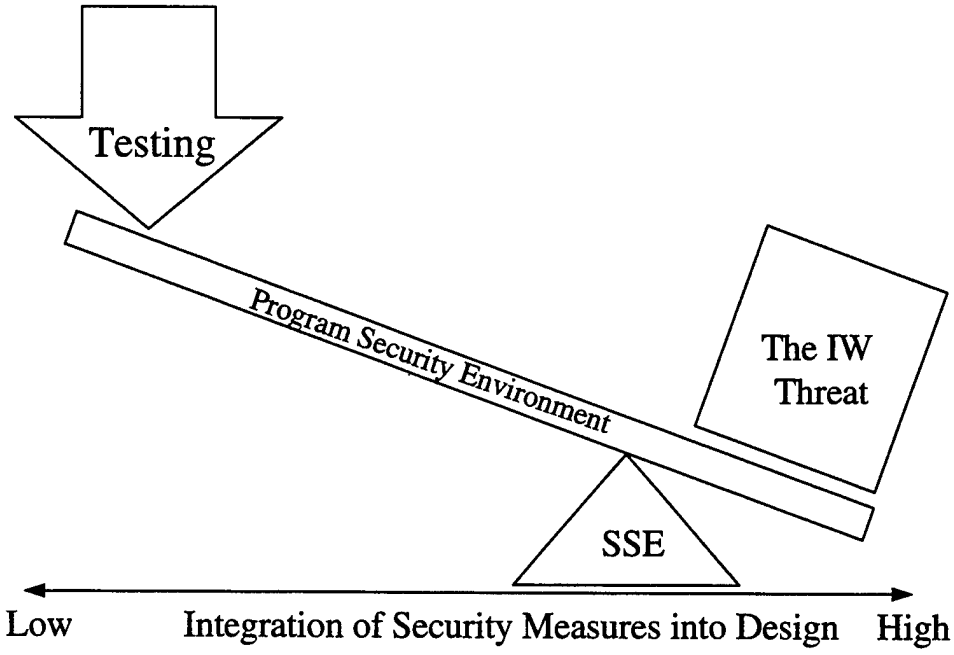

Figure 4-1, DIW Effort-Benefit Relationship

Figure 4-1 illustrates how improving the PSE (lengthening the lever) and moving the fulcrum closer to the load (integrating DIW measures into the design) increases the amount of work that can be performed against IW threats. Improving the PSE and integrating SSE into the systems engineering process become more important as the complexity of future weapons systems increase. The more complex the system the more likely that testing will not uncover design flaws and vulnerabilities. This is especially true with software intensive systems which cannot be adequately tested for the absence of defects or intentionally inserted malicious code. While testing is still an important part of

the system, over-reliance on comprehensive testing is expensive and not necessarily cost-effective. Like many other processes in the acquisition arena, attempting to inspect or test in quality are not usually the best courses of action. Only with a good PSE and better DIW integration can the contractors and the government be more confident that their systems are truly secure and combat ready.

Understanding where to apply resources to achieve the greatest DIW benefit is key to instituting an effective DIW plan. Using this knowledge a heuristic can be developed to assist in integrating DIW efforts into the defense systems acquisition process.

C. INFORMATION WARFARE VULNERABILITY REDUCTION HEURISTIC

The purpose of this section is to provide the acquisition decision-maker a tool to assist in assessing the IW threats to a system and identifying countermeasures to reduce the risk of successful IW attacks. It is designed to assist program managers in integrating DIW activities into the defense systems acquisition lifecycle management model. The heuristic is a derivative of the risk management process model published in Volume III of the C2 Protect Library and included as Figure 3-1 in Chapter III. It focuses strictly on the Vulnerability Assess/Fix part of the process. While it does not directly support quantitative cost-benefit analysis that is vital to the risk management process, previous analysis has shown generally where the greatest benefits are to be gained. Accurate quantitative analysis would require detailed intelligence regarding probability of attack and known or suspected enemy capabilities. However, armed with both this heuristic and

intelligence data a PM should be able to perform an adequate cost-benefit analysis using any one of several established methodologies.

It should be noted at this point that the successful application of this heuristic requires the use of the IPT concept. IW and systems security experts working alone cannot adequately analyze a major weapon system for all possible IW vulnerabilities. A group composed of experts from the different engineering areas and all the systems acquisition disciplines is required to develop a comprehensive vulnerability reduction plan.

The heuristic is primarily designed to assist in formulating a defense against attack for future exploitation conducted prior to a system's fielding or during a major post-deployment modification. This is the major threat not sufficiently addressed in the C2 Protect PMP. The heuristic helps to extend the C2 Protect Program to *all* defense systems. It also gives the PM a tool for filling in the details associated with the responsibilities outlined in the C2 Protect Library. In this way, it addresses the shortcomings of the Army's DIW plan.

This heuristic is of limited usefulness in combating direct program attacks. The key defense against this threat is a good, secure MIS. DOD 5000.2-R , the C2 Protect PMP and AR 380-19 provide adequate direction and guidance on information security requirements and standards. Additionally, mature, effective methods for assessing MIS vulnerabilities are available to PEOs/PMs and should be employed as early as possible after a PMO is established. However, the heuristic can augment these efforts by

identifying areas of specific concern that may require additional attention during various phases of a system's lifecycle.

The heuristic is simple and contains only four steps. A list of the steps and a detailed discussion of each follows:

1. Analyze the System

This is a non-trivial endeavor. There is a myriad of potential problem areas to consider: system function and processes, inputs and outputs, interfaces with other systems, COTS components, reliance on foreign technology or components, logistics support, user security requirements definition, required functionality and the amount of software, to name just a few. This process is the critical first step in combating IW attacks focused on inducing vulnerabilities for future exploitation. This analysis, coupled with the next step, may illuminate IW vulnerabilities in any or all of these areas.

2. Consider the IW Threats and Weapons

Once the IPT members have a clear understanding of a system's potentially vulnerable areas they can consider exactly how attacks for future exploitation or direct program attacks could be conducted. The IPT should also determine which IW weapons and techniques would most likely be used in the attacks. For example, the IPT should suspect that an adversary may wish to insert malicious software into a system. From this assessment the IPT may determine that the most vulnerable software components in the system are the communication device drivers and that a trojan horse or logic bomb are the

most likely weapons. This analysis completes the necessary groundwork and paves the way for developing an integrated action plan.

3. Develop and Map Countermeasures for each Threat to the Proper Acquisition Phase/Functional Area Combination

After the details of the IW threats are identified and documented, suitable countermeasures should be developed and integrated into the appropriate acquisition phase. The countermeasure plan should begin with a strategy for implementing IW actions required by existing regulations and directives. Next, each specific threat should be matrixed against the eight systems acquisition process disciplines and the countermeasures required in each discipline area identified. Also, additional measures may be identified by simply asking: "What can be done in this discipline area to improve the overall DIW posture of the program"? Not all countermeasures will be applicable in every phase of the acquisition process. The DIW actions should be integrated into the overall process by phase and discipline area. Primary responsibility for supervising the execution of the countermeasures can be assigned to the appropriate discipline area supervisors. This is also the step that helps strengthen a PMO's MIS security. This process identifies critical time frames when extra security on specific types of information may be warranted.

4. Refine and Monitor the Plan

The plan must be a living document. A system's design changes and more details are filled in as it progresses through the acquisition phases. Additional knowledge about the details of a system allow for greater refinement of the vulnerability reduction plan.

Along with the expected refinements that come from a more detailed engineering and design process, any number of other variables may require changes in the vulnerability reduction plan. User requirements may change. Congressional funding support levels may waver. The prime contractors often change between phases or additional contractors may be added during the production phase. All these actions require close monitoring from a program management perspective and now must also be monitored from an IW point of view.

D. GENERALIZED VULNERABILITY REDUCTION PLAN

This section contains a generalized example of the vulnerability reduction heuristic applied to a typical major weapons program. The plan will be presented in a matrix format by phase, acquisition discipline and threat. This format is intended to take advantage of the already established defense systems acquisition lifecycle management model which is often illustrated in a similar manner. This should assist acquisition professionals in understanding the heuristic and integration process. Due to space limitations the phases must be addressed in five separate tables beginning with the Table I, Pre-Milestone 0 DIW activities.

There are seemingly few acquisition tasks to be accomplished during the period prior to Milestone 0; however those included are extremely important. Ensuring that DIW considerations are an integral part of the requirements definition process is critical to producing a secure system. It is also the basis for producing accurate Requests for Proposal (RFPs) and other essential contracting instruments. Additionally, early consideration of DIW issues assists in establishing an accurate funding baseline.

A significant change in normal operating procedure is needed here to support these actions. At this point in a program a PMO has not yet been established. Most of the responsibility for accomplishing these actions will fall on the user. Non-acquisition agencies have the responsibility to educate the user about the IW threats that should be considered in the threat analysis during the MAA and MNS development process. However, the acquisition community must move to include itself earlier in the requirements definition process and assist the user in developing achievable DIW requirements.

Phase 0, Shown in Table II, gives the PM the chance to establish an atmosphere of security or a culture that 'thinks' DIW. The program is still very immature. Design details are almost non-existent, therefore specific technical vulnerabilities are not yet a major concern. This is the perfect opportunity for the PM to ensure that PMO personnel are properly trained, that sufficient IW expertise is part of the matrix support and that the PMO's information systems are in compliance with established standards.

Phase 0 also provides the first chance to influence contractors' business and development environment through the RFP and contract award process. This makes Phase 0 a critical period from an IW perspective. It is a great opportunity to firmly establish secure development processes as a component of the source selection criteria. Additionally, potential problems with proposed usage of COTS, or foreign sourced components can be evaluated.

	Attacks for Future Exploitation	Direct Program Attacks
Pre-Milestone 0		
Acquisition Management	Ensure that DIW issues are reflected in MNS.	Review program protect requirements and policies.
System Engineering	Assist in integrating DIW into requirements generation process and MNS.	
Software Acquisition Mgmt		
Test and Evaluation		
Manufacturing & Production		
Acquisition Logistics		
Financial Management	Include DIW measures in initial cost estimates.	Allow for program protect expenditures in budget.
Contract Management		

Table I, Pre-Milestone 0 DIW Activities

Table III illustrates actions that may be taken in Phase I: Program Definition and Risk Reduction. Phase I is when engineering and design functions really begin to shape the system. Once a concept has been chosen and more detailed design begins, the integration of SSE into the system engineering process becomes critical. IPTs and design reviews such as the System Requirements Review (SRR) and System Functional Review (SRR) are effective management tools that can assist in ensuring that proper DIW integration is taking place. Configuration management is essential as a guard against subversion of the design and engineering processes.

This is also an advantageous time for the PM to reassess the security of the PMO's information system, because during Phase II detailed design data and preliminary testing results will be produced and must be protected. Information system security flaws must be identified and corrected prior to Phase II.

Phase II, depicted in Table IV, is the most probable time for an adversary to insert malicious software or hardware. For this reason, maximum emphasis on establishing a secure software development environment and strict configuration management procedures is needed. It is important to note that DIW measure must continue even after testing and the system appears to be performing as designed and proven suitable for fielding. Stringent configuration management is still necessary after completion of testing. Adversaries will likely attempt to make modifications after testing to reduce the probability of detection.

This is also the time to ensure that all DIW features required by the ORD are part of the allocated product baseline. The Critical Design Review (CDR) is the established tool for accomplishing this task. This formal review evaluates the design for completeness. Traceability of DIW requirements to the product baseline should be added to the other established evaluation areas.

Phase III, shown in Table V, is the second most probable time for an enemy to make unauthorized modifications to a system. Strict production controls and safeguards on electronically formatted detailed design data are paramount, especially if second-sourcing or Pre-Planned Product Improvements (P^3Is) are part of the acquisition strategy.

	Attacks for Future Exploitation	Direct Program Attacks
Phase 0 Concept Exploration		
Acquisition Management	Consider DIW issues in determining most promising concept(s) and in requirements analysis. Incorporate C2 Protect Risk Mgmt process model Establish IW as integral part of IPT organization	Adhere to regulatory requirements in AR 380-19 & DOD 5000.2-R Assign program security responsibilities and provide adequate staffing and IW training.
System Engineering	Include IW in system threat assessment. Obtain SSE expertise through matrix support and ensure full integration into system engineering process. Establish strict standards for configuration management Ensure inclusion of adequate DIW requirements in ORD.	
Software Acquisition Mgmt	Review ORD for sufficient SW DIW requirements.	
Test and Evaluation	Include IW testing in preliminary TEMP.	Safeguard TEMP
Manufacturing & Production	Identify potential COTS, NDI or foreign source components for IW vulnerability evaluation.	
Acquisition Logistics	Consider IW when conducting supportability analysis	
Financial Management		Safeguard costing and budget data. Use most secure EDI system available. Carefully monitor EDI system for IW attack.
Contract Management	Ensure DIW requirements included in RFP. Use security of system development environment as a component of the selection criteria.	Use security of the contractor's corporate management information system as a component of the selection criteria.

Table II, Phase 0 DIW Activities

	Attacks for Future Exploitation	Direct Program Attacks
Phase I Program Definition & Risk Reduction		
Acquisition Management	Monitor integration of IW into IPT organization and procedures.	Continue to protect program information. Have Red Team conduct IW vulnerability assessment of PMO.
System Engineering	Use IPT concept to ensure DIW measures properly integrated into systems design. (SSE) Use design reviews to verify integration. Maintain strict configuration mgmt controls. Reassess IW threat.	
Software Acquisition Mgmt	Continue to monitor SW development environment. Ensure prototyped modules that may be included in final design meet system security requirements.	
Test and Evaluation	Include IW issues in TEMP. Conduct additional testing on SW and HW components identified as vulnerable, paying special attention to COTS, NDI and foreign components.	
Manufacturing & Production		
Acquisition Logistics		
Financial Management	Partially base progress payments on DIW efforts.	Continue to safeguard cost/budget data.
Contract Management	Use security of system development environment as a component of the selection criteria. Provide incentives for secure development environment.	Use security of the contractor's corporate management information system as a component of the selection criteria.

Table III, Phase I DIW Activities

	Attacks for Future Exploitation	Direct Program Attacks
Phase II Engineering & Manufacturing Development		
Acquisition Management	Continue to apply C2 Protect risk management process model.	Continue program protect efforts.
System Engineering	Ensure functional baseline includes DIW performance requirements. Continue strict configuration mgmt controls. Spot check specifications and TDP for unauthorized modifications. Reassess IW threat.	Safeguard detailed design specifications.
Software Acquisition Mgmt	Conduct final IW assessment of SW architecture. Monitor reuse library and test reused code for malicious SW. Continue security evaluation of SW development environment.	Safeguard SW cost and performance data.
Test and Evaluation	Focus DT&E efforts on components and code modules identified as vulnerable. Include Red Team in OT&E to simulate threat capabilities.	
Manufacturing & Production	Formulate production DIW plan to include prevention of unauthorized modifications or use of altered foreign source components. Include DIW measures in Production Readiness Review.	Formulate DIW plan to prevent IW attacks aimed at slowing production or affecting quality.
Acquisition Logistics	Guard logistics system from modification of spare parts or corruption of electronic orders	Guard against alteration of reliability data during testing.
Financial Management	Make progress and incentive payments partially based on DIW effort.	Monitor EDI system for attacks. Safeguard cost and budget data.
Contract Management	Continue to make DIW posture a selection criterion and offer incentives for good DIW posture.	Continue to make secure MIS a selection criterion.

Table IV, Phase II DIW Activities

	Attacks for Future Exploitation	Direct Program Attacks
Phase III Production, Fielding/Deployment & Operational Support		
Acquisition Management	Continue to apply C2 Protect risk management process model. Monitor system performance.	Continue program protect efforts.
System Engineering	Ensure SSE is part of ECP and major modification process. Reassess IW threat.	
Software Acquisition Mgmt	Maintain secure SW development environment for maintenance and modification functions.	
Test and Evaluation	Conduct follow-on OT&E as new IW threats emerge.	
Manufacturing & Production	Execute production DIW plan. Consider security measures for technical data transfer if second sourcing.	Execute production DIW plan.
Acquisition Logistics	Spot check repair parts lots for modifications. Monitor selection of spare parts vendors. Monitor reliability data for performance problems.	
Financial Management	Make progress and incentive payments partially based on DIW effort.	Monitor EDI system for attacks. Safeguard cost and budget data.
Contract Management	Continue to make DIW posture a selection criterion and offer incentives for good DIW posture.	Continue to make secure MIS a selection criterion.

Table V, Phase III DIW Activities

This example is overly simplified due to the lack of system specifics. Without system details it is impossible to include technical solutions to specific design vulnerabilities. Therefore, only management-oriented actions are presented in any detail.

However, when viewed as a top-level template, it provides a useful framework upon which to build a detailed vulnerability reduction plan. It supplements the previous analysis by highlighting the interdependencies between the discipline areas and need for vulnerability reduction planning to be a continuous process, executed throughout a system's lifecycle, if it is to effectively counter the IW threat. It also leads to the conclusion that contractor efforts are key in fighting the IW threat. The importance of contractor involvement and other conclusions stemming from this research will be discussed in Chapter V.

V. SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

A. SUMMARY

Information warfare is a growing concern for military, government and industry leaders. Studies continue to identify numerous IW vulnerabilities in the NII and DII. Information warfare represents a significant threat to our military, because of its reliance on the largely unsecure information infrastructures and information intensive weapons systems.

The military, government and the commercial sector, to a lesser extent, have begun working diligently to reduce their IW vulnerabilities, each making progress in its perceived areas of concern. Their efforts have been somewhat hampered by the unique characteristics of IW. The Army, for its part, has responded to the threat by formulating a defensive IW plan (the C2 Protect Program) that focuses on the threat of tactical IW operations.

The Army acquisition community has an important and difficult role to play in support of the Army's DIW plan. Army acquisition programs must ensure that future systems are less vulnerable to IW than their predecessors. In order to accomplish this mission, the acquisition community must accomplish three tasks. First, DIW measures must be integrated into the requirements definition process. Second, the PMO must guard the system against malicious alterations to software and hardware. Third, program information and program management processes must be protected from IW attacks.

The current acquisition environment makes these tasks even more difficult to accomplish. The prevailing acquisition strategy is to reduce costs and shorten procurement cycle times by reducing oversight and relying on COTS or NDI solutions whenever possible. Actions needed to strengthen a system's DIW mechanisms are often in direct conflict with these methods. Finally, there is no existing DIW planning framework for acquisition decision-makers.

B. CONCLUSIONS

This research shows that integrating DIW efforts into the defense systems acquisition process model is an effective methodology for countering *all* IW threats to new systems and for managing IW risks. This research also demonstrates that actions taken in the acquisition process can reduce the vulnerability of future systems to IW.

The old adage "An ounce of prevention is worth a pound of cure," is quite applicable here. The vulnerability reduction plan produced by following the heuristic described in Chapter IV will assuredly prevent vulnerabilities from being built into a system by omission and greatly reduces the probability of vulnerabilities being maliciously introduced into a system. This emphasis on prevention instead of the iterative find-and-fix solution is the best way to build a strong IW defense and meet budget constraints. The only problem is that within the acquisition process the Army only owns about one-quarter of that "ounce". The civilian defense contractors own the other three-quarters. For this reason, contract management is an extremely important tool in combating IW. The Army must influence contractors through awards and incentives to establish secure development environments and high-assurance development processes,

because it can no longer dictate processes and oversight as it previously did through MILSPECS and MIL-STDS. Contract management is also a weak link, because DIW has never before been considered when writing contracts.

C. RECOMMENDATIONS

Based on the conclusions reached as a result of this research, three actions are recommended. First, the IW risk management process model from Volume III of the C2 Protect Library (Figure 3-1) should be modified to indicate that the threat may directly attack the system and not just influence the system through the Operational Architecture. (Figure 5-1).

Second, the heuristic described in Chapter IV should be adopted by the Army acquisition community as a tool in implementing the IW risk management process model and for reducing IW vulnerabilities in future systems. A prerequisite for this action would be the formal integration of the IW risk management process model into the Army acquisition process. Modifications to AR 70-1 should be made to make this recommendation operational. This action should be executed as a pilot program used to evaluate the suitability of the IW vulnerability reduction heuristic and IW risk management process model for adoption throughout DOD.

Lastly, procedures for incentivizing desirable DIW actions should be developed and immediately instituted in applicable contracts. Measures of Performance (MOP) and past performance indicators of DIW tasks for use in source selection must be developed or identified. Possible candidates for MOPs or past performance indicators include: Capability Maturity Model (CMM) evaluations, incorporation of excepted

development standards for high integrity software such as the National Institute of Standards and Technology (NIST) SP 500-223, use of automated assurance tools such as *Unravel,* or results from IW vulnerability evaluations conducted by independent consultants or government agencies.

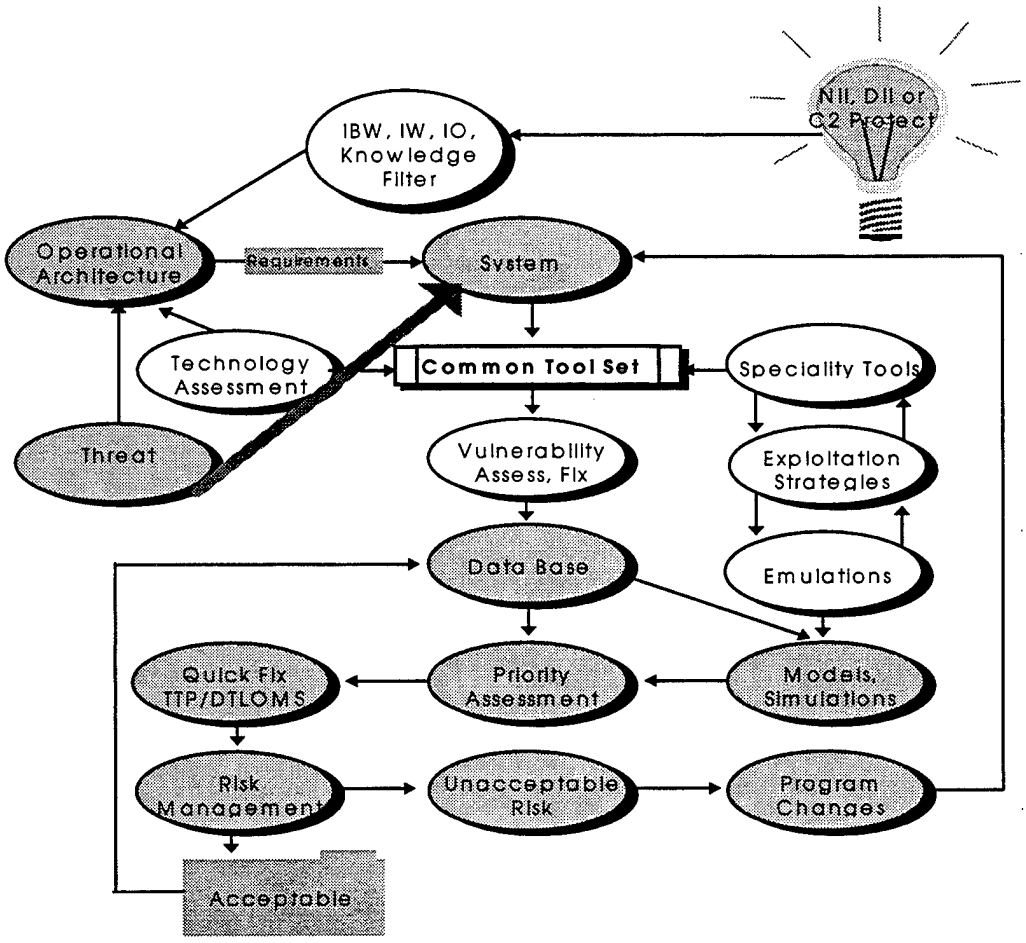

Figure 5-1, IW Risk Management Process Model after (Vol. III ,C2 Protect Library, 1996)

D. RECOMMENDATIONS FOR FURTHER STUDY

1. Software Reuse Library Security

Investigate security measures established by government and civilian software developers to prevent unauthorized modifications to code in their reuse libraries. Determine if the measures are strong enough to prevent damage to our defense systems.

2. Software Assurance Techniques

Examine techniques, methodologies and tools used by software developers to certify and accredit software and software development tools. Determine which practices result in the best quality, most secure software. Evaluate these practices, tools, techniques and methodologies for effectiveness in discovering intentionally inserted malicious code. Compare these best practices to typical defense contractor software development and validation processes.

3. Contract Management's Role in DIW

Research how contracts should be structured to assist Program Managers' efforts to reduce the vulnerability of systems to IW. This research should focus on establishing DIW posture as a source selection criterion, incentives for secure development processes and subcontract management issues.

4. Information Warfare Strategy, Policy and Organization

Investigate the decision-making process for IW strategy and policy. Examine organizational IW responsibilities, structure and chain-of-command for effectiveness. Determine whether or not the acquisition community can properly support the IO strategy from within the current organizational framework. If Secretary Perry's statement that

technological breakthroughs are changing the face of war and how we prepare for it, then it follows that our organizational processes and structure must also change.

APPENDIX - ACRONYMS AND ABBREVIATIONS

AAE	Army Acquisition Executive
ACAT	Acquisition Category
ADO	Army Digitization Office
AIS	Automated Information System
ASD(RDA)	Assistant Secretary of the Army for Research, Development & Acquisition
BOS	Battlefield Operating Systems
CECOM	Communications and Electronics Command
CERT	Computer Emergency Response Team
CDR	Critical Design Review
CIO	Chief Information Officer
COMSEC	Computer Security
COTS	Commercial Off-The-Shelf
C2	Command and Control
C2PWG	Command and Control Protect Working Group
C2W	Command and Control Warfare
C3	Command, Control, Communications
C4	Command, Control, Communication and Computers
DA	Department of the Army
DCSINT	Deputy Chief of Staff for Intelligence
DCSOPS	Deputy Chief of Staff for Operations
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISC4	Director of Information Systems for Command, Control, Communications and Computers
DIW	Defensive Information Warfare
DOD	Department of Defense
DODD	Department of Defense Directive
DT&E	Developmental Test and Evaluation
EIW	Economic Information Warfare
EMP	Electromagnetic Pulse
EW	Electronic Warfare
GAO	Government Accounting Office
HERF	High Energy Radio Frequency

IBW	Information Based Warfare
IO	Information Operations
IOT&E	Initial Operational Testing and Evaluation
IPT	Integrated Process Team
ISS	Information Systems Security
ISSRP	Information Systems Security Resource Plan
IW	Information Warfare
LFT&E	Live-Fire Testing & Evaluation
LRIP	Low-Rate Initial Production
MAA	Mission Area Analysis
MILSPEC	Military Specification
MILSTD	Military Standard
MIS	Management Information System
MNS	Mission Needs Statement
MOP	Measures of Performance
NCSC	National Computer Security Center
NDI	Non-Developmental Item
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
ODCSOPS	Office of the Deputy Chief of Staff for Operations
ODISC4	Office of the Director of Information Systems for Command, Control, Communications and Computers
ORD	Operational Requirements Document
OT&E	Operational Testing & Evaluation
PEO	Program Executive Officer
PM	Program Manager
PMP	Program Management Plan
PSYCW	Psychological Warfare
P3I	Pre-Planned Product Improvement
RDA	Research, Development and Acquisition
RDT&E	Research, Development Testing and Evaluation
RFP	Request for Proposal
SFR	System Functional Review
SPO	Special Projects Office
SRR	System Requirements Review
STA	System Threat Analysis

LIST OF REFERENCES

Department of Defense, Department of Defense Regulation 5000.2-R Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs, Washington, D.C., GPO, 15 March 1996.

Department of Defense, Department of Defense Directive (DODD) 5000.1 Defense Acquisition, Washington, D.C., GPO, 15 March 1996.

Department of the Army, Army Regulation 380-19 Information Systems Security, Washington, D.C., 1 August 1990.

Department of the Army, Army Regulation 70-1 (Revised Draft) Army Acquisition Policy, Army Material Command, 17 October, 1996.

Garigue, Robert, "Information Warfare, Developing a Conceptual Framework," World Wide Web, URL http://moowis.cse.dnd.ca/%7Eformis/overview/iw, 1996.

Irvine, Cynthia, "Report on the Defensive Information Warfare Symposium, New Orleans, Louisiana, 11-12 December, 1995.

Jones, Edward, "Differences in Specifying 'What to Test' Parameters for Hardware and Software," Army RD&A, September-October 1996.

Libicki, Martin, "What is Information Warfare," World Wide Web, URL http://www.ndu.edu/ndu/actpubs/act003/a003ch02.html, 1995.

Loranger, Phillip J., Chairperson, C2 Protect Working Group, Telephone Interview, November, 1996.

Magsig, Daniel E., "Information Warfare in the Information Age," World Wide Web, URL http://www.seas.gwu.edu/student/dmagsig/infowar.html, 1995.

McAuliffe, Amy, "PowerPC rolls along with M1A2 Upgrade Design-In", Military & Aerospace Electronics, January, 1996.

Office, Director of Information Systems for Command, Control, Communications and Computers, The Army Command and Control Protect Library, Volume I, Program Management Plan, Washington, D.C., August, 1995.

Office, Director of Information Systems for Command, Control, Communications and Computers, The Army Command and Control Protect Library, Volume II, Master Training, Washington, D.C., 29 February, 1996.

Office, Director of Information Systems for Command, Control, Communications and Computers, The Army Command and Control Protect Library, Volume III, Implementation Plan, Washington, D.C., 29 February, 1996.

Rabb, Craig P., Department of the Army Civilian, Research and Development Project Leader, CECOM RDEC IEWD, Email Correspondence, November 1996 - February 1997.

Reimer, Dennis J., General, USA, Chief of Staff of the Army, CSA Message "Information Operations Strategy," Washington, D.C., 3 September, 1996.

Russell, Deborah and Gangemi, G.T. Sr., Computer Security Basics, First Edition, O'Reilly & Associates, Inc., California, 1992.

Stone, Mark, Associate Professor, Department of Systems Management, Naval Postgraduate School, Personal Interview, 4 December, 1996.

Waldschmidt, Bruce, Policy Chief, OASA (RDA), Telephone Interview, November, 1996.

Waller, Douglas, "Onward Cyber Soldiers," Time, August 24, 1995.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Fort Belvoir, Virginia 22060-6218

2. Dudley Knox Library, Code 013 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, California 93943-5101

3. OASA (RDA) 1
   ATTN: SARD-ZAC
   103 Army Pentagon
   Washington, DC 20310-0103

4. Dr. Keith Snider, Code SM/Sk 3
   Department of Systems Management
   Naval Postgraduate School
   Monterey, California 93943

5. Dr. Dan Boger, Code SM/Bo 1
   Department of Systems Management
   Naval Postgraduate School
   Monterey, California 93943

6. Dr. Mark Stone, Code SM/St 1
   Department of Systems Management
   Naval Postgraduate School
   Monterey, California 93943

7. Dr. Carl Jones, Code SM/Js 1
   Department of Systems Management
   Naval Postgraduate School
   Monterey, California 93943

8. Dr. Fred Levien, Code IW/Lv 1
   Information Warfare Academic Group
   Naval Postgraduate School
   Monterey, California 93943

9. Mr. Craig P. Rabb.....1
Director, USA CECOM, RDEC, IEWD
ATTN: R&T Div (Mr. Rabb)
Mail Stop 41, VHFS
Warrenton, VA 20187-5100

10. MAJ William S. Mullis.....2
10402 Independence Lane
Little Rock, AR 72209